Java集合

【5/5】详细描述HashMap的扩容机制（触发条件、rehash过程）。

**Java7扩容条件：**

元素数量超过阈值 && 发生哈希冲突

**Java8扩容条件：**

1. 情况一：元素数量超过阈值
2. 情况二：链表长度≥8 && 数组长度＜64，优先扩容而不是转为红黑树

Rehash过程**：**

1. 新建一个2倍大小的数组
2. 只需部分移动：if e.hash & oldCap==0
   1. 0接在loTail后面
   2. 1接在hiTail后面

基础：

数组长度是2的次方，且扩容为2倍。

**oldCap**：

位运算代替取模提高效率、保证hash均匀分布：hash & (数组长度-1)

旧长16即010000，16-1=15即001111

新长32即100000，32-1=31即011111

rehashing时用**旧长16**即010000作为一个Mask看对应该位是否为1

源码**if e.hash & oldCap==0**（0接在loTail后面、1接在hiTail后面）

​

【3/3】HashMap底层结构是什么？如何解决哈希冲突？

**HashMap底层结构**是数组+链表，Java8后引入红黑树。

当链表长度≥8且 数组容量≥64时，链表会转换为红黑树  
（链表长度≤8时，链表性能足够且内存占用低）

当红黑树节点数≤6时，红黑树会退化为链表

**解决哈希冲突**：

1. **拉链法**
2. **红黑树**
3. **二次扰动函数：**如果哈希值低位变化较小，计算索引时，低位相同的键会映射到同一位置。**将哈希值高位低位异或、优化索引分布、减少哈希冲突**
4. **动态扩容机制：**
   1. 超过阈值（容量×负载因子，默认0.75）扩容2倍并重新计算索引。
   2. 0.75是空间利用与哈希冲突的最佳平衡  
      负载因子过高会增加哈希冲突  
      **负载因子**过低则导致频繁扩容

【3/3】为什么HashMap线程不安全？举例说明并发问题场景。

**HashMap线程不安全的原因：**

数组数据覆盖、头插环形链表、红黑树树化结构异常

**解决方案：**

1. Collections.synchronizedMap(new HashMap<>())：在方法级别加锁，性能低
2. ConcurrentHashMap：采用分段锁（7）或CAS+ synchronized（8），性能高。

【2/2】HashMap的遍历方式有哪几种？哪种效率更高？

1. ​entrySet() 效率最高、推荐使用。
2. forEach()+ Lambda 底层实现基于entrySet()。
3. ​keySet() 返回所有键的集合，通过 map.get(key)获取值
4. values() 返回所有值的集合。由于无法通过值获取键

for (Map.Entry<String, Integer> entry : map.entrySet()) {

String key = entry.getKey();

Integer value = entry.getValue();

System.out.println(key + ": " + value);

}

map.forEach((key, value) -> {

System.out.println(key + ": " + value);

});

Java并发

【5/5】CAS的原理是什么？存在哪些缺陷？

**CAS（Compare And Swap）**由 CPU 硬件指令保证原子性的无锁并发​：

比较当前值（V）与预期值（E），相等则将新值（N）写入，否则不操作。

1. ​ABA 问题：值从 A 变为 B 再变回 A，CAS 无法感知中间变化

* ​解决：版本号或时间戳

1. ​自旋开销：如果 CAS 失败，线程会不断自旋重试、消耗 CPU

* ​解决：限制自旋次数。

1. ​单变量限制：无法直接支持多个变量的原子操作。

* ​解决：封装为复合操作。

【5/5】AQS的核心机制是什么？举一个基于AQS实现的工具类。

AQS（Abstract Queued Synchronizer）抽象队列式锁为构建锁和同步器提供框架

核心机制：

1. ​通过 state表示**资源状态（ReentrantLock通过 state 记录锁的重入次数）**
2. ​使用​CLH 队列（双向链表）​实现自旋锁的公平排队。

* 在 CLH 队列中，线程会按照请求顺序排队，因此后面请求锁的线程不会抢先获得锁。线程会自旋等待，直到它前面的线程释放锁，这就保证了公平性。
* 通过 CLH 队列，线程被强制按照队列顺序获取锁，避免了线程饥饿的现象，保证了每个线程都有机会在合适的时间获得锁。

1. 线程通过 acquire() 和 release() 方法进入或离开队列。

提供 tryAcquire() 和 tryRelease() 等模板方法，由子类实现具体逻辑。

【4/4】ConcurrentHashMap如何实现线程安全？Java7和Java8的区别？

​

Java7分段锁（默认16个段）：锁粒度大（段级别），性能低

Java8CAS + synchronized：锁粒度小（桶级别），性能高

【3/3】为什么ConcurrentHashMap的size()方法需要特殊处理？

1. 并发更新导致的不准确
2. 直接遍历的性能开销

分段累加、多次统计：  
分别统计每个 Segment 的元素数量再累加。  
通过多次统计，如果结果一致则返回，否则重试。

【3/4】synchronized和ReentrantLock的性能对比？

**synchronized**：

JVM内置优化，适合低竞争

隐式锁 自动获取释放

**ReentrantLock**：

基于AQS，适合高竞争

显式锁 手动获取释放

支持中断锁、尝试锁等特性

。

SpringBoot / SSM

【5/5】Spring AOP的实现原理？JDK动态代理和CGLIB的区别？

Spring AOP​通过动态代理实现：

* JDK动态代理​
  + 基于接口、通过 Proxy 类生成代理对象
  + 无法代理未实现接口的类
* CGLIB代理​
  + 基于继承、通过字节码生成子类代理
  + 无法代理 final 类或方法

【4/5】Spring Bean的生命周期和作用域有哪些？

**Bean生命周期：**

1. ​实例化
2. ​属性赋值
3. ​初始化

* ​**前置处理**postProcessBeforeInitialization()。
* ​Initialization**()**：
  + @PostConstruct注解方法
  + InitializingBean的afterPropertiesSet()
  + init-method
* ​**后置处理**postProcessAfterInitialization()

1. ​使用
2. ​销毁

* @PreDestroy注解方法
* DisposableBean的destroy()
* destroy-method

**Bean的作用域：**

Singleton 默认单例

Prototype 每次请求创建一个新的Bean实例。

Request 每个HTTP请求创建一个Bean实例

Session 每个HTTP会话创建一个Bean实例

Application 每个ServletContext生命周期内创建一个Bean实例

WebSocket 每个WebSocket会话创建一个Bean实例

【3/4】SpringBoot自动配置的实现机制（@EnableAutoConfiguration）？

1. ​@SpringBootApplication =   
    @SpringBootConfiguration

+ @EnableAutoConfiguration // 关键：开启自动配置

+ @ComponentScan  
Spring Boot启动时，AutoConfigurationImportSelector 通过 SpringFactoriesLoader 机制，加载 META-INF/spring.factories 中定义的 自动配置类。扫描META-INF/spring.factories，加载自动配置类。

1. ​条件匹配@Conditional：根据类路径、配置文件、Bean是否存在判断是否加载配置类。
   1. @ConditionalOnClass
   2. @ConditionalOnMissingBean

【5/5】如何解决循环依赖问题？三级缓存机制详解。

循环依赖**：**两个或多个Bean相互依赖，导致无法完成初始化。

三级缓存**：**

1. ​一级缓存（Singleton Objects Map 单例对象）：  
   存放已经实例化、属性注入、初始化的 Bean。
2. 二级缓存（Early Singleton Objects Map 早期对象）：  
   存放已实例化，但未完成属性注入和初始化的 Bean。  
   防止 AOP每次调用ObjectFactory.getObject()都产生新代理对象。
3. 三级缓存（Singleton Factories Map 单例工厂）：  
   ObjectFactory的getObject()调用getEarlyBeanReference()创建早期Bean。

**解决循环依赖的**流程**：**

1. ​**Bean实例化**：

* 创建Bean实例，但未注入属性和初始化。
* 将Bean工厂对象（ObjectFactory）放入三级缓存。

1. ​**属性注入**：

* 发现依赖的Bean，尝试从一级缓存获取。
* 如果一级缓存不存在，从二级缓存获取。
* 如果二级缓存不存在，从三级缓存获取工厂对象，将这个 ObjectFactory 从三级缓存中移除，生成的Bean并放入二级缓存。

1. ​**Bean初始化**：

* 完成属性注入和初始化。
* 将Bean从二级缓存移除，放入一级缓存。

【3/4】Spring事务失效的常见场景有哪些？

1. ​异常类型不匹配  
   默认只回滚RuntimeException和Error，如果抛出比如IOException且未配置rollbackFor，不会回滚。
2. ​异常没抛出
3. ​同类方法调用  
   同一个类中，方法A调用方法B（B有@Transactional），实际调用的是原始对象的方法，而不是代理对象的方法，而事务管理是通过代理机制实现的，B的事务不会生效。
4. ​非public方法、final方法、static 方法
5. ​多线程调用：事务基于ThreadLocal实现，多线程事务无法传递。
6. ​其他
   * **事务传播行为**PROPAGATION\_NOT\_SUPPORTED会挂起事务
   * 未正确配置数据源DataSourceTransactionManager
   * MyISAM引擎本身不支持事务
   * 非Spring管理Bean

【4/4】MyBatis的#和$的区别及SQL注入问题。

* #：预编译、更安全
* $：直接拼接、存在SQL注入风险

动态表名、排序字段必须用$。因为表名、字段名、ORDER BY 排序字段等 SQL 结构 不能使用 ? 作为参数绑定。只有值（变量）可以用 # 作为参数占位符。

由于 $ 存在 SQL 注入风险，我们需要严格控制用户输入，确保只能传递合法的表名和字段名（白名单校验/使用 Enum 限制可选字段）

【4/5】SpringMVC请求处理流程中的HandlerAdapter作用？

1. DispatcherServlet接收请求
2. HandlerMapping查找处理器  
   根据请求URL找到对应Controller
3. HandlerAdapter适配并调用处理器
   * 1. 选择合适的适配器执行
     2. 通过handle()方法执行业务逻辑
4. Controller   
   执行业务逻辑，返回ModelAndView或数据对象
5. HandlerAdapter处理返回值：  
   将ModelAndView或数据对象转换为适合视图解析器的格式。
6. DispatcherServlet返回响应  
   将处理后的渲染视图或JSON数据返回给客户端。

【3/3】SpringBoot如何集成Tomcat容器？

默认内嵌Tomcat容器

* **端口**：8080
* **最大连接数**：10000  
  TCP 连接的数量，即有多少个客户端可以连接到服务器。
* **最大线程数**：200  
  可用的工作线程，表示服务器可以同时处理多少个请求。

MySQL

【4/5】B+树索引的查询过程？为什么不用哈希索引？

**B+树索引的查询过程：​**

从根节点逐层比较确定下一层子节点的位置最终定位到叶子节点

如果是范围查询，叶子节点通过链表连接，可以高效地遍历满足条件的数据。

**为什么不用哈希索引？**

1. ​B+树叶子节点有序排列，适合顺序访问和范围查询  
   哈希索引随机分布，只能等值查询
2. ​哈希冲突影响查询性能
3. 频繁插删时成本高

【3/4】事务隔离级别和MVCC的实现原理？

**事务隔离级别：​**

1. ​读未提交：可能脏读
2. ​读已提交：可能不可重复读
3. ​可重复读​：可能出现幻读
4. ​串行化：串行执行避免所有并发问题但性能最低

**MVCC实现原理：​**

1. ​根据事务ID和版本时间戳判断哪些数据可见
2. ​读操作不会阻塞写操作，写操作生成新版本，旧版本仍可被其他事务读取。
3. ​定期清理不再被任何事务引用的旧版本数据，释放空间。

【2/2】Redo Log和Undo Log的作用及写入机制？

**Redo Log（重做）：​**记录“做了什么”，用于崩溃恢复。

* 事务提交先将修改写入Redo Log Buffer。
* 将Redo Log Buffer刷新到磁盘。

**Undo Log（回滚）：​**记录“如何撤销”，用于回滚和MVCC。

* 事务修改数据前先将旧数据写入Undo Log。
* Undo Log存储在专门的段中。

【2/3】覆盖索引和索引下推的区别？

覆盖索引**（Covering Index）：​**

查询所需的所有字段都包含在索引中，无需回表查询主键或数据行。

适用于SELECT只查询索引字段

索引下推**（Index Condition Pushdown, ICP）：​**

在存储引擎层利用索引过滤数据，减少回表次数。

适用于WHERE条件中包含索引字段和非索引字段的查询。

【3/4】死锁的产生条件及排查方法（show engine innodb status）

**死锁的产生四大条件：​**

1. ​互斥**条件**：资源一次只能被一个事务占用。
2. ​占有**并等待**：事务持有资源的同时，等待其他资源。
3. ​不可剥夺：已分配的资源不能被强制剥夺，只能由持有者释放。
4. ​循环等待：事务之间形成资源等待的环路。

**排查方法：​**

1. ​运行SHOW ENGINE INNODB STATUS;。
2. ​查找LATEST DETECTED DEADLOCK部分

* 查看涉及的事务ID。
* 分析事务持有的锁和等待的锁。
* 定位造成循环等待的SQL语句。

1. ​调整事务逻辑（如锁顺序、事务粒度、重试机制）

【1/2】Change Buffer对写操作的优化原理？

* ​​延迟写入：当修改非唯一二级索引时，先将修改记录到Change Buffer中，不直接写入磁盘。
* ​批量合并：当相关索引页被加载到内存时，再将Change Buffer中的修改合并到索引页。

适用于写多读少、非唯一二级索引的场景。

【4/5】分库分表后全局ID生成方案有哪些？

1. ​UUID：本地生成

* 无序

1. ​Snowflake算法：64位ID = 时间戳 + 机器ID + 序列号。

* 时钟回拨可能引发问题

1. 数据库自增ID：每个库/表设置不同的自增起始值和步长

* 依赖数据库。

1. ​Redis自增ID：利用Redis的原子操作（如INCR）生成全局ID。

* 依赖Redis，存在单点故障风险。

1. ​号段模式（Segment）​：从数据库预分配一批ID号段，本地缓存使用。

* 号段用尽需重新申请，可能短暂阻塞。

【1/5】主从同步延迟的解决方案？

1. ​**优化主库性能**：优化SQL语句，减少锁争用和大事务。
2. ​**优化从库性能**：开启并行复制
3. ​**减少网络延迟**：主从库部署在同一机房或低延迟网络环境。
4. ​半同步复制，确保主库提交时至少一个从库已接收日志
5. ​分库分表
6. ​读写分离

Redis

【3/5】Redis单线程模型为什么能高效处理请求？

1. ​内存读写速度极快。
2. ​内置高效的数据结构（如哈希表、跳表）
3. 多路复用技术（如epoll），单线程可以同时处理多个客户端请求。
4. ​无需考虑多线程并发控制，减少锁竞争和上下文切换开销。
5. ​基于事件驱动模型，高效处理网络事件和定时任务。

【4/5】缓存雪崩/穿透/击穿的解决方案？

Redis缓存穿透：

穿透不存在：指查询一个不存在的数据，缓存中没有相应的记录，每次请求都会去数据库查询，造成数据库负载激增。

* 使用布隆过滤器，过滤掉不存在的请求，避免直接访问数据库。
* 对不存在的数据缓存一个标识，以减少对数据库的请求。

Redis缓存击穿：

击穿热点：指某个热点数据在缓存中过期，导致大量请求同时访问数据库，造成数据库负载激增。

* 使用互斥锁，确保同一时间只有一个请求可以去数据库查询并更新缓存。
* 热点数据永不过期。

Redis 缓存雪崩：

多个雪崩：指多个缓存数据在同一时间过期，导致大量请求同时访问数据库，造成数据库负载激增。

* 双缓存策略：主缓存设置短过期时间，备份缓存设置较长过期时间
* 随机过期时间

【3/5】RDB和AOF的优缺点及混合持久化机制？

RDB（快照）：

* ​直接加载快照文件，恢复效率高。
* **文件紧凑体积小**，便于备份和传输。

AOF（追加日志）：

* ​记录每次写操作，数据完整性高。
* ​AOF文件是文本格式，**便于人工检查和修复**。

混合持久化机制：

先用RDB生成快照，然后追加AOF日志

* ​恢复效率高：优先加载RDB快照。
* ​数据完整性高：AOF日志补充了RDB快照后的数据变化。

【2/5】Redis Cluster的slot分配算法？

Redis Cluster将整个键空间划分为16384个哈希槽（Slot）**​**，每个槽对应一个哈希值范围。

1. 适配 CRC16 算法，让哈希值均匀映射到槽。  
   CRC16 算法的结果是 16 位的，取值范围是 0 到 65535。16384 是 65536 的四分之一，使用 16384 个哈希槽可以让 CRC16 的哈希值在取模后能较为均匀地分布在各个槽中，充分利用哈希值的空间，减少哈希冲突的概率。
2. 优化网络传输，方便集群管理与维护。  
   在节点之间传递关于哈希槽分配的信息时，用较少的比特位就可以表示一个哈希槽的状态，使得消息体相对较小，从而减少网络传输的开销，提高集群的通信效率和性能。

分配算法**：​**

1. ​对每个键计算CRC16哈希值，然后对16384取模，得到对应的slot编号。
2. ​Redis Cluster每个节点负责一部分slot。当集群节点增减时，slot可以动态重新分配，确保负载均衡。

【2/5】大Key问题如何定位和解决？

定位：​

1. ​使用Redis自带的MEMORY USAGE命令或RedisInsight监控工具分析Key的内存占用。
2. ​通过SCAN结合STRLEN、HLEN、LLEN等命令，遍历所有Key统计Key的大小。
3. ​通过慢查询日志（slowlog）定位访问频率高或耗时的Key。

解决：​

1. ​将大Key拆分多个小Key  
   为大Key设置合理过期时间
2. ​对Value进行gzip压缩  
   避免存储过大的Value，改用分页或分段加载
3. ​冷热分离、冷数据存储到磁盘

【2/4】布隆过滤器的实现原理及误差率计算？

布隆过滤器是一个由m个二进制位组成的位数组，初始值全为0。使用k个独立的哈希函数，将元素映射到位数组的k个位置，将对应的位数组位置置为1。**查询元素**时，通过k个哈希函数计算，若有任意位置为0，则元素一定不存在。



【2/4】Redis事务和Lua脚本的原子性区别？

Redis事务通过MULTI、EXEC、DISCARD命令实现

* 批量执行，不具备完全原子性
* 事务执行期间，其他客户端命令可能会插入执行
* 如果某条命令失败，后续命令仍会执行，不支持回滚

Lua脚本​通过EVAL或EVALSHA执行

* 真正的完全原子操作
* 执行期间完全隔离，其他客户端命令会被阻塞
* 不支持回滚但可以通过逻辑控制实现类似效果

【2/5】热Key问题的解决方案（本地缓存/分片）？

热Key访问频率极高，导致Redis单节点负载过高，影响性能和稳定性。

**解决：​**

1. ​本地缓存**：​**在应用层缓存热Key的值，减少对Redis的直接访问。
2. ​分片**：​**将热Key分散到多个节点，通过哈希算法或手动分片均衡负载。
3. ​读写分离：将读请求分散到从节点，减轻主节点压力。
4. ​缓存预热：提前加载热Key到缓存，避免高峰期的集中访问。
5. ​限流降级：对热Key的访问进行限流，防止系统过载。

计算机网络

【2/5】TCP三次握手的详细过程和状态变化？

三次握手

* 第一次: 客户端发出同步请求报文。
* 第二次：服务器发出同步确认报文。
* 第三次: 客户端发出确认报文。



四次挥手

* 第一次：客户端发出连接释放报文。
* 第二次：服务器发出确认报文。
* 第三次：服务器发出连接释放确认报文。
* 第四次：客户端发出确认报文。



【1/4】HTTP1.0和HTTP1.1的区别是什么？

1. 持久连接

* **HTTP1.0**：每次请求都需要建立一个新的TCP连接，响应之后关闭连接。
* **HTTP1.1**：默认启用持久连接（Connection: keep-alive），允许多次请求/响应复用同一连接，减少了建立和关闭连接的开销。

2. 管道化

* **HTTP1.0**：不支持请求管道化，每次请求必须等待前一个请求完成。
* **HTTP1.1**：支持请求管道化，客户端可以在等待响应的同时发送多个请求，但服务器端必须按顺序返回响应。

3. 缓存控制

* **HTTP1.0**：缓存控制较为简单，仅依赖于Expires头部。
* **HTTP1.1**：新增了Cache-Control头部，提供了更细粒度的缓存控制，例如no-cache、no-store、max-age等。

4. Host头部

* **HTTP1.0**：不包含Host头部，无法在多个域名共享同一IP时进行区分。
* **HTTP1.1**：强制要求在请求中包含Host头部，允许同一IP托管多个虚拟主机（即多个域名）。

5. 错误代码

* **HTTP1.0**：错误码较少，错误响应不够细致。
* **HTTP1.1**：新增了多个错误码，如：
  + 409 Conflict：表示请求与当前状态冲突。
  + 410 Gone：表示资源已永久删除等。

【1/4】HTTP2.0与HTTP1.1相比有哪些主要改进？

1. 多路复用

* **HTTP1.1：虽然支持管道化，但请求和响应仍然是串行化的，且如果其中一个请求被阻塞，其他请求也会受到影响。**
* **HTTP2.0：使用一个连接复用多个请求和响应，消除了HTTP1.1中的队头阻塞问题，使得请求和响应可以并行传输。**

2. 头部压缩

* **HTTP1.1：头部信息未压缩，且请求头较为冗长，这增加了网络带宽的消耗。**
* **HTTP2.0：采用HPACK算法对HTTP头进行压缩，减少了冗余数据的传输，尤其对于重复的请求头，如Cookies等，效果显著。**

3. 流量控制

* **HTTP1.1：没有内建流量控制，主要依赖TCP的拥塞控制，可能导致带宽浪费。**
* **HTTP2.0：支持对每个流进行独立的流量控制，服务器和客户端可以通过调整流的大小来管理带宽使用。**

4. 服务器推送

* **HTTP1.1：只有客户端可以发起请求，服务器只能被动响应，无法主动推送资源。**
* **HTTP2.0：服务器可以在客户端请求之前主动推送资源，这对于加载复杂页面时有显著的性能提升。例如，在请求HTML文件的同时，服务器可以主动推送该页面依赖的CSS、JavaScript文件等。**

5. 二进制协议

* **HTTP1.1：是基于文本的协议，易于人类阅读和调试，但由于解析过程繁琐，性能不如二进制协议。**
* **HTTP2.0：采用二进制协议，而不是文本协议，数据以帧的形式传输，解析更高效。**

【1/4】HTTP3.0有了解过吗？它与之前的版本有哪些主要不同？

1. 基于QUIC协议

* **HTTP1.x 和 HTTP2**：两者都依赖于TCP协议，TCP的连接建立和管理较为复杂且容易受到延迟影响。
* **HTTP3.0**：HTTP3不再依赖TCP，而是基于QUIC协议（Quick UDP Internet Connections）。QUIC是Google提出的一个新协议，建立在UDP之上，具有低延迟和更好的多路复用性能。

2. 零RTT连接建立

* **HTTP1.x 和 HTTP2**：这两个版本都使用基于TCP的三次握手过程，每次建立新连接都需要等待完整的握手。
* **HTTP3.0**：QUIC协议支持零RTT连接建立（0-RTT），即客户端在首次发送请求时，可以立即开始数据传输，而无需等到完整的三次握手过程结束。通过保存会话信息，可以减少延迟。

3. 避免队头阻塞

* **HTTP2**：虽然支持多路复用，但仍然受TCP队头阻塞的影响。当一个流的数据包丢失时，整个连接的延迟会增加，影响其他流的传输。
* **HTTP3.0**：QUIC协议为每个HTTP请求分配独立的流，所有流之间互不阻塞。即使某个流发生丢包或延迟，其他流依然能够继续传输数据，从而避免队头阻塞。

4. 内建加密

* **HTTP2**：虽然支持TLS加密，但并没有内建，使用时需要显式配置TLS层。
* **HTTP3.0**：QUIC将TLS加密内建于协议中，每个QUIC数据包都会自动加密，不需要额外的TLS握手过程。

5. 头部压缩

* **HTTP1.1**：HTTP1.1没有内建头部压缩功能，导致大量重复头部信息的传输，浪费带宽。
* **HTTP3.0**：与HTTP2类似，HTTP3继续使用HPACK进行头部压缩，提高了带宽效率。

【2/5】HTTPS和HTTP有哪些区别？

**1**. 端口号

* **HTTP**：默认为80端口。
* **HTTPS**：默认为443端口，通信是加密的，增加了一个安全层。

2. 加密和传输层

* **HTTP**：数据在传输过程中是未加密的，容易被拦截、篡改。
* **HTTPS**：通过SSL/TLS协议进行加密，使得数据在传输过程中即使被截获，也无法解密。

【2/5】HTTPS工作原理是什么？它是如何实现数据加密的？

1. SSL/TLS协议

* **SSL/TLS**协议是实现HTTPS加密通信的核心技术，TLS是SSL的继任版本。SSL/TLS用于加密数据传输、验证身份并确保数据完整性。TLS提供了对称加密、非对称加密和哈希算法的结合，确保数据在传输中的机密性、完整性和认证。

2. 加密过程

* **非对称加密**：用于密钥交换和身份认证。非对称加密使用公钥和私钥对数据进行加解密，公钥加密的数据只能用对应的私钥解密。
* **对称加密**：HTTPS使用对称加密算法（如AES）对传输的数据进行加密。对称加密的优点是加密和解密速度快，但问题是密钥的安全性。因为双方使用相同的密钥加密和解密数据，必须确保密钥的安全传输。

3. SSL/TLS握手过程

1. **客户端Hello**：客户端向服务器发送支持的加密算法、生成的随机数等信息。
2. **服务器Hello**：服务器从客户端提供的算法中选择一个并返回自己的数字证书（包含公钥），以及用于生成会话密钥的随机数。
3. **密钥交换**：客户端使用服务器的公钥加密生成的会话密钥，然后发送给服务器。服务器使用自己的私钥解密，获得会话密钥。
4. **验证身份**：客户端验证服务器的数字证书，以确保与预期的服务器通信，防止中间人攻击。
5. **完成握手**：客户端和服务器使用协商的会话密钥进行加密通信。

4. 数据传输

* **加密数据传输**：一旦握手完成，客户端和服务器就开始使用对称加密算法（如AES）加密通信数据。此时，通信双方使用的是会话密钥（由握手过程中的密钥交换生成），确保数据在传输过程中既不会被窃取，也不会被篡改。
* **数据完整性**：在数据传输过程中，SSL/TLS协议使用哈希算法（如SHA-256）对数据进行完整性验证，确保数据在传输过程中没有被篡改。

【1/5】HTTPS的TLS握手过程（ECDHE算法）？

1. ​**Client Hello：​**  
   客户端发送支持的TLS版本、加密套件列表和随机数。
2. ​**Server Hello：​**  
   服务器选择TLS版本、加密套件，并发送随机数。
3. ​**Server Certificate：​**  
   服务器发送证书，证明其身份。
4. ​**Server Key Exchange：​**  
   服务器发送ECDHE参数（椭圆曲线公钥），并签名。
5. ​**Server Hello Done：​**  
   服务器通知客户端初始消息发送完毕。
6. ​**Client Key Exchange：​**  
   客户端生成ECDHE参数（椭圆曲线公钥），发送给服务器。
7. ​**Key Derivation：​**  
   客户端和服务器使用ECDHE参数生成对称密钥。
8. ​**Change Cipher Spec：​**  
   双方切换到加密通信模式。
9. ​**Finished：​**  
   双方发送加密的Finished消息，验证握手完整性。

【1/5】TIME\_WAIT状态的作用及过多时的解决方案？

**TIME\_WAIT状态的作用：​**

1. 确保TCP连接的四次挥手正确完成，防止旧连接的延迟数据包干扰新连接。
2. 保证对端收到最后的ACK，避免连接关闭异常。

**TIME\_WAIT过多的解决方案：​**

1. 调整内核参数：减少net.ipv4.tcp\_tw\_reuse和net.ipv4.tcp\_tw\_recycle（注意：tcp\_tw\_recycle在较新内核中已弃用）。
2. 增加可用端口范围：扩大net.ipv4.ip\_local\_port\_range。
3. 使用连接池：复用连接，减少频繁创建和关闭。
4. 优化应用逻辑：减少短连接的使用。

【2/5】TCP快速重传和超时重传的区别？

**快速重传：**

1. **触发条件：**收到3个重复ACK（表明后续数据包丢失）。
2. **响应速度：**更快，依赖重复ACK立即重传。
3. **适用场景：**适用于部分数据包丢失，网络状况较好时。

**超时重传：**

1. **触发条件：**发送数据包后，未收到ACK且重传计时器超时。
2. **响应速度：**较慢，依赖计时器超时。
3. **适用场景：**适用于严重丢包或连接中断。

【1/5】QUIC协议如何解决队头阻塞问题？

1. ​**基于UDP：​**避免了TCP层的队头阻塞。
2. ​**多路复用：​**在单个连接上并行传输多个独立的流，每个流的数据包丢失不会影响其他流。
3. ​**独立流控制：​**每个流有自己的流量控制和重传机制，互不干扰。
4. ​**快速重传和恢复：​**QUIC在应用层实现快速重传，减少数据包丢失对整体传输的影响。

【1/5】TCP拥塞控制中的BBR算法原理？

1. ​**核心思想：​**  
   瓶颈带宽与往返传播时间（Bottleneck Bandwidth and Round-trip propagation time, BBR）通过动态测量网络带宽和最小往返时间来优化发送速率，避免传统基于丢包的拥塞控制算法的缺点。
2. ​**关键步骤：​**

* ​**Startup：​** 快速探测可用带宽，指数增长发送速率。
* ​**Drain：​** 排空队列，降低发送速率至稳定状态。
* ​**Probe Bw：​** 周期性探测带宽变化，调整发送速率。
* ​**Probe RTT：​** 周期性测量最小RTT，更新RTprop。

1. ​**优势：​**

* 避免缓冲膨胀（Bufferbloat）。
* 在高带宽、高延迟网络中表现更佳。

【1/5】WebSocket协议如何实现全双工通信？

1. **​基于HTTP/HTTPS握手：​**

* 客户端通过HTTP/HTTPS发送Upgrade请求，协商切换到WebSocket协议。
* 服务器响应确认，完成协议升级。

1. **​持久化连接：​**

* 建立TCP连接后WebSocket保持连接打开，避免HTTP的短连接开销。

1. **​数据帧传输：​**

* 使用轻量级二进制帧格式，支持双向数据传输。
* 客户端和服务器可以随时主动发送数据，无需等待请求-响应模式。

1. **​低延迟：​**

* 数据传输无需HTTP头部开销，减少通信延迟。

操作系统

【1/5】进程和线程的区别？协程的优势是什么？

进程：是资源分配的基本单位，一个进程可以包含多个线程

进程有独立的上下文（代码、数据、文件）等，创建和切换开销大

进程之间是相互独立的，需要进程间通信（IPC）机制，如管道、消息队列、共享内存、套接字等

线程：是CPU调度的基本单位，属于进程

线程组内共享资源，但有独立的PC和堆栈，创建和切换开销较小

线程直接读写内存即可，但需要同步机制以避免数据竞争

【2/5】虚拟内存的作用及页面置换算法（LRU实现）？

**虚拟内存的作用：**

* ​**扩展**：允许程序使用比物理内存更大的地址空间。
* ​**隔离**：每个进程拥有独立的虚拟地址空间，提高安全性。
* ​**管理**：简化内存分配和回收，支持动态内存需求。
* ​**共享**：多个进程可以共享同一块内存区域。

**页面置换算法（LRU实现）：**

1. ​**LRU（Least Recently Used）​**：淘汰最久未使用的页面。
2. ​**实现方式**：

* ​**链表法**：维护一个链表，最近使用的页面在头部，最久未使用的在尾部。每次访问页面时，将其移动到链表头部，淘汰时移除尾部页面。
* ​**计数器法**：为每个页面维护一个计数器，记录最近使用的时间戳，淘汰时选择时间戳最小的页面。

【1/5】select/poll/epoll的区别及边缘触发模式？

1. ​**select**：

* 使用 ​fd\_set 数据结构，支持的文件描述符数量有限（通常 1024）。
* 每次调用需要遍历所有文件描述符，效率低。
* 时间复杂度：O(n)。

1. ​**poll**：

* 使用 ​pollfd 数组，支持的文件描述符数量无限制。
* 和 select 一样需要遍历所有文件描述符，效率低。
* 时间复杂度：O(n)。

1. ​**epoll**：

* 使用事件驱动机制，只关注活跃的文件描述符，效率高。
* 支持边缘触发（ET）和水平触发（LT）模式。
* 时间复杂度：O(1)。

**边缘触发模式（ET）：**

* ​只在状态变化时通知一次，需一次性处理所有数据，否则会丢失事件。
* ​**优点**：减少事件通知次数，提高效率。
* ​**适用**：高性能、高并发的网络编程。

【1/5】用户态和内核态切换的开销来源？

1. ​**上下文切换**：保存和恢复 CPU 寄存器、程序计数器等状态。
2. ​**权限级别切换**：用户态和内核态之间的权限级别切换。
3. ​**缓存失效**
4. ​**系统调用开销**：系统调用需要经过内核验证和处理，增加额外时间。
5. ​**中断处理**：切换可能伴随中断处理，进一步增加开销。

【1/3】自旋锁在单核CPU下是否有意义？

**无意义**

* 自旋锁的核心是忙等待，在单核 CPU 下持有锁的线程无法被抢占，其他线程无法获得 CPU 时间，导致死锁或资源浪费。
* 单核 CPU 更适合使用阻塞锁（如互斥锁），让等待线程主动让出 CPU。

【1/4】内存映射（memory map, mmap）系统调用的实现原理？

1. ​mmap系统调用将文件/设备映射到进程的虚拟地址空间，实现文件读写或共享内存。
2. ​**实现步骤**：

* ​**创建映射**：内核在进程的虚拟地址空间中分配一段区域，建立虚拟内存与文件/设备的映射关系。
* ​**延迟加载**：映射时不立即加载文件内容，而是通过缺页中断按需加载。
* ​**读写操作**：进程通过指针直接访问映射区域，内核负责将数据同步到文件或设备。
* ​**解除映射**：调用 munmap 时，释放虚拟地址空间并同步数据到文件。

1. **优点**：减少用户态和内核态的数据拷贝，提高性能。

【1/5】进程间通信共享内存和消息队列的对比？

**共享内存**：

* ​原理：多个进程映射同一块物理内存，直接读写数据。
* ​优点：速度快，无数据拷贝。
* ​缺点：需要同步机制（如信号量）避免竞争。
* ​适用场景：高性能、大数据量通信。

**消息队列**：

* ​原理：内核维护消息队列，进程通过发送/接收消息通信。
* ​优点：自带同步机制，无需额外处理竞争。
* ​缺点：速度较慢，有数据拷贝开销。
* ​适用场景：小数据量、异步通信。

【1/5】零拷贝技术（sendfile）的实现原理？

零拷贝技术（sendfile）在文件传输中，让内核直接将文件数据从磁盘读取到网络缓冲区，无需经过用户态，避免数据在用户态和内核态之间的拷贝，提升性能。

* 传统方式：磁盘 -> 内核缓冲区 -> 用户缓冲区 -> 网络缓冲区
* sendfile ：磁盘 -> 网络缓冲区

Linux命令

【3/5】如何用grep查找包含"error"的日志并统计次数？

* grep "error" logfile.log：查找 logfile.log 中包含 "error" 的所有行
* grep -c "error" logfile.log：统计 logfile.log 中包含 "error" 的行数

【3/5】awk如何实现按列求和？

awk '{sum+=$3} END{print sum}' filename

* {sum+=$3}：逐行累加第3列的值。
* END{print sum}：处理完所有行后，输出累加结果。

【3/5】如何用sed批量替换文件中的字符串？

sed -i 's/old\_string/new\_string/g' filename

* sed：Stream Editor 流编辑器
* -i：in-place，直接原地修改文件、不输出到终端
* s：**替换命令**，格式为 s/查找内容/替换内容/
* g ：全局替换

【2/5】strace和perf工具的作用及使用场景？

strace：跟踪进程系统调用

strace -p <pid> 监视进程 <pid> 的所有系统调用。

perf：分析 CPU 性能瓶颈、函数调用链、硬件事件

perf top 实时查看占用 CPU 最高的函数

【2/5】如何用tcpdump抓取指定端口的SYN包？

tcpdump -i eth0 'tcp[tcpflags] & tcp-syn != 0 and port 80'

* -i eth0：指定网卡接口
* tcp[tcpflags] & tcp-syn != 0：匹配 SYN标志位
* port 80：指定端口